COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
AUDITOR-CONTROLLER

March 5, 2014

TO: Marvin Southard, D.S.W., Director
Department of Mental Health

FROM: Wendy L. Watanabe
Auditor-Controller

SUBJECT: **HIPAA AND HITECH ACT COMPLIANCE REVIEW – ROYBAL FAMILY MENTAL HEALTH CENTER**

We have completed a review of the Department of Mental Health (DMH) Roybal Family Mental Health Center's (RFMHC) compliance with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic Clinical Health (HITECH) Act.[1] Our review was prompted by prior findings of non-compliance during unannounced site visits to RFMHC. On January 30, 2014, we provided your Department with our final draft report, and your Department agreed with our findings. No exit conference was requested. This report includes our findings, recommendations for corrective action, and your Department's response.

Approach/Scope

On November 21, 2013, we conducted an unannounced visit to RFMHC as part of our effort to ensure that the County's HIPAA covered programs and clinics are posting their Notice of Privacy Practices (NPP) in prominent patient locations, as required. We noted that RFMHC did not post the NPP. In addition, the facility manager was unaware of the NPP standard, indicating a lack of management knowledge and accountability for core HIPAA requirements. These findings prompted a full HIPAA compliance review of RFMHC.

Our review evaluated RFMHC's compliance with the HIPAA Privacy Rule and DMH's HIPAA policies and procedures. We also used the *HIPAA Privacy Rule and Health Information Technology for Economic Clinical Health (HITECH) Act Audit Tool* in evaluating their compliance. DMH management is responsible for establishing and maintaining effective internal compliance with HIPAA regulations, and has oversight of

[1] 45 Code of Federal Regulations (CFR) Parts 160 and 164

the HIPAA program throughout their facilities. We considered DMH's internal controls over their compliance program, and the HIPAA Privacy Rule requirements that could have a direct and material effect on RFMHC.

Our review covered the Privacy Rule requirements for:

- NPP for protected health information (PHI)
- Safeguards for PHI
- Training
- Complaint process
- Refraining from intimidating or retaliatory acts
- Uses and disclosures requiring authorization
- Accounting for disclosures of PHI
- Minimum necessary standard
- HITECH Act Breach Notifications

Results of Review and Recommendations

Notice of Privacy Practices

The HIPAA Privacy Rule requires a covered entity with direct treatment relationships with individuals to give the NPP to every individual no later than the date of first service delivery, and to make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. If the provider maintains an office or other physical site where care is provided directly to individuals, the provider must also post the notice in the facility in a clear and prominent location where individuals are likely to see it, as well as make the notice available to those who ask for a copy.[2]

In our follow-up review, RFMHC management reported that all patients are given the NPP on their first service delivery date. We reviewed five randomly selected patient charts, and noted they all included the required acknowledgement of receipt. In addition, we toured the facility and noted that the facility posted the NPP in English and Spanish, on the registration window in the waiting area, where patients and visitors are likely to see it.

While RFMHC was not in compliance with the NPP standard at the time of our unannounced site visit, the facility has addressed the deficiencies in this area, and was fully compliant at the time of this review.

[2] Ibid., §164.520(c)

Safeguards for Protected Health Information

A covered entity must have in place appropriate administrative, physical, and technical safeguards to protect the privacy of PHI. A covered entity must reasonably safeguard PHI and electronic PHI, and make reasonable efforts to prevent any intentional or unintentional use or disclosures that violate the Privacy Rule.

RFMHC management reported that their computers are protected by endpoint protection software, which blocks downloading of PHI or other data to portable storage devices. Computers are configured to prevent workforce members from saving PHI onto their hard drives. RFMHC management further stated that medical charts are stored in the lockable cabinets in its own storage room inside the business office; and, charts are distributed by clerical staff to the employees' lockable cubbies for their appointments. RFMHC management reported that the facility relied on an honor system in tracking that the medical charts are returned at the end of the business day.

During our site visit, we noted that the two computer monitors, located inside the business office, were in plain view of patients that may be standing near the registration window, which may lead to incidental or prohibited disclosures of PHI.

While we confirmed that the medical records are kept in a storage room inside the business office, the storage room is left unlocked, and a copier used by the entire workforce is located in the medical records storage room, resulting in significant and unnecessary access to the area where PHI is stored. Additionally, RFMHC management stated that custodians who service the facility have keys to access the storage room.

Based on these findings, it appears that RFMHC has not implemented reasonable safeguards for PHI.

Recommendations

1. **Roybal Family Mental Health Center management ensure that all outbound medical charts are properly tracked and returned to the medical records room at the end of the business day.**

2. **Roybal Family Mental Health Center management ensure that medical records room is properly secured by restricting access to areas where protected health information is stored to those employees who have a business need (i.e. relocate the copier and only allow custodians to enter the storage area with the assistance from authorized staff).**

3. **Roybal Family Mental Health Center management implement reasonable safeguards in the business office to ensure that the computer monitors are not in plain view of the patients or visitors.**

RFMHC management indicated that they are in agreement with our recommendations and have begun implementing corrective actions to address our recommendations.

Training

RFMHC, as a HIPAA covered program, must train all members of its workforce on policies and procedures related to PHI as required by the HIPAA Privacy and Security Rules, as well as retraining staff when regulations are updated, to the extent necessary and appropriate for them to do their jobs. Workforce members include employees, volunteers, and trainees.

DMH Human Resources is responsible for ensuring its workforce members are trained on HIPAA compliance via the Learning Net. RFMHC management is responsible for training workforce members on DMH's HIPAA policies and procedures, and additional role-based training for their workforce members when applicable.

We reviewed RFMHC training records, and found that 20 out of 38 workforce members (52%) have not completed the required HIPAA training, which includes recent updates to the HIPAA regulations. While one of the non-compliant employees is on family leave, and would be expected to complete the required training upon returning to work, RFMHC management did not have a business reason for failing to train the remaining 19 employees. Based on these findings, it appears that RFMHC is not fully complying with the HIPAA training standards.

Recommendation

4. **Roybal Family Mental Health Center management ensure that all workforce members complete the updated HIPAA training.**

RFMHC's response indicates that they implemented plans to ensure all non-compliant employees complete the required HIPAA training.

Complaint Process

A covered entity must provide a process for patients to complain about its policies and procedures. In addition, a covered entity must document all complaints received and their disposition, if any.

RFMHC management informed us that patient complaints are handled in accordance with DMH Policy Number 500.11, *HIPAA Privacy Complaints*. Patients are directed to

contact the Program Head, who is the facility's privacy coordinator, or the DMH Patients' Rights Office to file a complaint.

We observed that the DMH NPP posted in the waiting area informs patients that they may file a complaint with the U.S. Department of Health and Human Services (HHS), the County's Chief HIPAA Privacy Officer (CHPO), or the DMH Patients' Rights Office. We also verified that HIPAA complaint forms were available in the waiting area. It appears that the RFMHC complaint process complies with HIPAA standard.

Refraining from Intimidating or Retaliatory Acts

Discussions with RFMHC management confirm they are aware of their obligation to comply with DMH Policy Number 500.18, *Refraining from Retaliatory or Intimidating Acts Against Individuals That Assert Rights Under HIPAA*. They also understand that the Office for Civil Rights (OCR) will investigate complaints against a covered entity that assert retaliatory actions. In the past year, no complaints related to retaliatory or intimidating acts were filed with the CHPO by RFMHC patients. It appears that RFMHC is in compliance with the non-retaliation standard.

Uses and Disclosures Requiring Authorization

OCR defines an authorization as a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose PHI to a third party specified by the patient. An authorization must specify a number of elements, including: (1) a description of the PHI to be used and disclosed, (2) the person authorized to make the use or disclosure, (3) the person to whom the covered entity may make the disclosure, (4) an expiration date, and (5) the purpose for which the information may be used or disclosed.

RFMHC management reported that they follow DMH policy 500.1, *Use and Disclosure of Protected Health Information Requiring Authorization*. We reviewed the policy and the authorization form and determined that they meet the Uses and Disclosures Requiring Authorization standard. Our review of two completed authorization forms from our randomly selected patient charts showed that the forms were properly filled out. It appears that RFMHC workforce members are trained and adhering to the uses and disclosures requiring authorization standard.

Accounting for Disclosures of Protected Health Information

The Privacy Rule gives patients the right to request and receive an accounting of all disclosures of their PHI made by the covered entity, with certain exceptions, for up to six years after the disclosure. The following disclosures of PHI are excluded from the accounting requirement: (1) to the patient, (2) for treatment, (3) for payment and health

care operations, (4) for facility directories, (5) pursuant to authorization, (6) pursuant to a limited data set agreement, (7) to persons involved in the patient's care, (8) for correctional institutions, and (9) for certain law enforcement purposes. In addition, an accounting of disclosures' log must be maintained in each patient's medical chart.

RFMHC management reported that they follow DMH policy 500.6, *Accounting of Disclosures of Protected Health Information,* to track all non-routine disclosures. However, our review of two completed accounting of disclosures logs, provided by RFMHC management, noted that workforce members did not appear to have a clear understanding of the information that should be tracked. Specifically, staff documented disclosures of PHI for treatment purposes, and when the facility received PHI from another covered entity, despite that these types of disclosures are exempt from the accounting requirement. DMH needs to ensure that RFMHC managers and employees are properly trained on accounting for disclosures of PHI.

Recommendations

5. **Department of Mental Health privacy officers provide guidance to Roybal Family Mental Health Center management on the Accounting of Disclosures of Protected Health Information standard.**

6. **Roybal Family Mental Health Center management ensure that workforce members are re-trained on the Department of Mental Health policy 500.6, Accounting of Disclosures of Protected Health Information.**

RFMHC management agrees with our recommendations. DMH's Privacy Officers provided re-training on Accounting of Disclosures of Protected Health Information to RFMHC management and staff.

Minimum Necessary Rule

When using, disclosing, or requesting PHI from another covered entity, the Privacy Rule requires a covered entity to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. OCR provides covered entities with flexibility to address their unique circumstances, and make their own assessment of what PHI is necessary for a particular purpose. Discussions with RFMHC management indicate that workforce members are aware of the minimum necessary standard.

HITECH Act Breach Notification

HHS issued regulations requiring health care providers to notify patients when their health information is breached. Specifically, health care providers and other covered entities must promptly notify affected patients of a breach, as well as the HHS Secretary

and the media in cases where a breach affects more than 500 patients. Breaches affecting fewer than 500 patients will be reported to the HHS Secretary annually. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate. Further, HHS' Breach Notification regulations emphasize the importance of ensuring that all workforce members are appropriately trained and knowledgeable about what constitutes a breach and on the policies and procedures for reporting, analyzing, and documenting a possible breach of unsecured PHI.

RFMHC management informed us that while they have not experienced a breach in their program, the workforce members are aware that they must report all incidents involving suspected or actual breaches to their immediate supervisors, who will report to the DMH Privacy Officer. We reviewed DMH policy 500.28, *Responding to Breach of Protected Health Information,* and it shows clear guidelines to workforce members in the event a breach or suspected breach of PHI is discovered.

Conclusion

We provided our findings and recommendations to DMH and RFMHC management on January 30, 2014. Overall, our review indicates that while there were areas of non-compliance, RFMHC management has initiated substantial efforts to comply with the HIPAA Privacy Rule regulations, as indicated by the attached correction plans dated December 20, 2013 and February 14, 2014. The DMH Privacy Officer should continue to work with and assist RFMHC management to address the deficiencies noted in our review, and report additional corrective actions taken or pending to the HIPAA Compliance Office within 120 days from the receipt of this report. We thank DMH's Privacy Officers and RFMHC managers and staff for their cooperation and assistance during this review.

Please call me if you have any questions, or your staff may contact Linda McBride, Chief HIPAA Privacy Officer, at (213) 974-2166.

WLW:RGC:GZ:LTM:JC

Attachments

c: William T Fujioka, Chief Executive Officer
John F. Krattli, County Counsel
Robert Pittman, Chief Information Security Officer, Chief Information Office
Judith Weigand, Compliance Officer, Department of Mental Health
Veronica Jones, Privacy Officer, Department of Mental Health
Ginger Fong, Privacy Officer, Department of Mental Health
Audit Committee
Health Deputies

COUNTY OF LOS ANGELES – DEPARTMENT OF MENTAL HEALTH
Roybal Family Mental Health Center

Facility HIPAA correction plan
December 20, 2013

MEDICAL ROOM ACCESS:

The medical records room will be restricted only to staff with a business need. Staff presently uses a FAX machine as well as a network copier/printer in the medical records office. The copier/printer will be moved to room 216 if a suitable data link is available. This is projected to be completed by January 31, 2014

No staff except supervisors and clerical shall have access to client charts. Staff requiring charts for clients they are assigned to, will request the chart from clerical, which will place the chart in the locked records cubicles facing west. Clinical staff has keys for the cubicles which are to remain locked at all times.

Until redesign of the records room ensures that all PHI is locked and secure, the evening cleaning staff will not have access to the records room. Additional locking cabinets and keys are being arranged before cleaning staff will be given access; this will be completed by December 31, 2013. Clerical staff assigned to the records office must keep the medical chart cabinets locked at all times until the fax/copier/printer is relocated, and thereafter, the medical records room will need to be monitored during working hours and restricted only to employees that have a business need.

Presently, RFMHC has only one key for the locking file cabinets in the records room. Two additional keys will be ordered. The three keys will be in possession of the program head, the outpatient/triage supervisor and the clerical team lead.

MEDICAL RECORDS TRACKING:

Clerical staff will use clinician's Outlook schedules to pull charts. Staff requiring additional charts, will request these with clerical assigned to the records room. Clerical will log the chart out. As charts are returned, clerical will mark their return on the Outlook print out or the chart request form. The clinic switchboard operator will continue to make reminder calls 30 minutes before closing to ensure that all charts are returned to the Records room for secure filing.

HIPAA TRAINING FOR NEW HIRES/TRANSFERS/VOLUNTEERS

Supervisors will include HIPAA training in the orientation for each new employee or volunteer, before they have any access to PHI. This will involve the material used in the on-line-training, and will include a short quiz to ensure that new staff understands the key concepts. Management will use a tracking log to ensure the staff complete the on-line training as well, within the first 30 days.

UPDATED HIPAA TRAINING FOR EXISTING EMPLOYEES

All Roybal employees who have not completed the updated on-line HIPAA training have been identified and instructed to be certified by January, 17, 2014. These are employees whose

certification predates April, 2013. This instruction was given on December 18, 2013, with a 30 calendar day window due to the holiday season. All supervisors have been given a list to track which employees must complete the training by the target date.

LOS ANGELES COUNTY DEPARTMENT OF MENTAL HEALTH
550 S. VERMONT AVE., LOS ANGELES, CA 90020 HTTP://DMH.LACOUNTY.GOV

MARVIN J. SOUTHARD, D.S.W.
Director
ROBIN KAY, Ph.D.
Chief Deputy Director
RODERICK SHANER, M.D.
Medical Director

February 14, 2014

To: Julia Chen, MA
Assistant HIPAA Privacy Officer
Los Angeles County, Department of Auditor-Controller

From: Ginger Fong
Privacy Officer, Compliance Program
Los Angeles County, Department of Mental Health (LAC-DMH)

Subject: HIPAA and HITECH Act Compliance Review
Roybal Family Mental Health Center (RFMHC)

This is our response to the Auditor-Controller's Draft report concerning compliance with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) at Roybal Family Mental Health Center (RFMCH).

Auditor-Controller Recommendation #1:
RFMHC management ensures that all outbound medical charts are properly tracked and returned to the medical records room at the end of the day.

RFMHC Response:
RFMHC agrees with Auditor-Controller's recommendation.
RFMHC management ensures that all outbound medical charts are properly tracked and returned to the medical records room at the end of the day by implementing the following procedures:

- Clerical staff pulls charts in the morning, based on each clinician's schedule and places these in the clinician's locked records box.
- Clinical staff can request additional charts by filing a request, which is logged by the clerical staff who obtains the chart for them.
- As charts are returned, they are checked off the clinician's schedule or off the chart request log.
- Clerical staff broadcasts a reminder to return all charts 30 minutes before the clinic closes.

Auditor-Controller Recommendation #2:
RFMHC management ensure that medical records room is properly secured by restricting access to area where protected health information is stored to those

employees who have a business need (i.e., relocate the copier and only allow custodians to enter the storage area with the assistance of the authorized staff.)

RFMHC Response:
RFMHC agrees with Auditor-Controller's recommendation.
RFMHC management ensures that the medical records room is properly secured and restricting access to only those employees who have a business need where protected health information is stored, by implementing the following procedures:

- All RFMHC staff has been instructed to follow established procedures for access to client charts.
- Each morning, charts are pulled by support staff and placed in clinicians' locked boxes.
- Each evening, all charts are returned to Medical Records to be properly secured in a locked cabinet before closing.
- The copy machine will be moved outside of the medical records room to avoid unnecessary traffic.

Auditor Controller Recommendation #3:
RFMHC management implement reasonable safeguards in the business office to ensure that the computer monitors are not in plain view of patients or visitors.

RFMHC Response:
RFMHC agrees with Auditor-Controller's recommendation.
RFMHC management implemented the following reasonable safeguards in the business office to ensure that the computer monitors are not in plain view of the clients or visitors:

- The door to the business office is closed at all times.
- A Special Request has been submitted for the 19" privacy screens that will further veil PHI from visitor views.

Auditor-Controller Recommendation #4:
RFMHC management ensures that all workforce members complete the updated HIPAA training.

RFMHC Response:
RFMHC agrees with Auditor-Controller's recommendation.
RFMHC management ensures that all workforce members have completed the updated HIPAA training. Most of the workforce members completed the HIPAA training.

- Thirty-five of the thirty-nine RFMHC staff and volunteers have updated certification that they have completed HIPAA version 3.
- Of the four outstanding staff, two currently lack access to the Learning Net and the web-based training. A Help Desk ticket has been opened with CIOB, to gain access to the Learning Net for these staff; until then, they have been given the

HIPAA policies and have reviewed them with their supervisors. Of the remaining two, one is on extended sick leave, and the other is on FMLA leave. Supervisors have been instructed to ensure completion of these trainings as soon as possible for these four staff members.

- A monitoring log has been created to remind supervisors where their staff members are regarding first time or renewal HIPAA training on an ongoing basis.

Auditor-Controller Recommendation #5:
LAC-DMH privacy officers provide guidance to RFMHC management on DMH Policy 500.6, Accounting for Disclosures of Protected Health Information standard.

RFMHC Response:
RFMHC agrees with Auditor-Controller's recommendation.
Management of RFMHC has received guidance from the LAC-DMH Privacy Officers on DMH Policy 500.6, Accounting for Disclosures of Protected Health Information standard.

- LAC-DMH Privacy Officers responded by telephone and e-mail to specific issues requiring further clarifications for the in-house training on February 5, 2014.
- In the future, any questions regarding Accounting of Disclosures of Public Health Information will be addressed with the LAC-DMH Privacy Officers, and responses will be disseminated by management to all RFMHC staff via written communications and trainings.

Auditor-Controller Recommendation #6:
Roybal Family Mental Health Center management ensures that workforce members are re-trained on DMH Policy 500.6, Accounting of Disclosures of Protected Health Information.

RFMHC Response:
RFMHC agrees with Auditor-Controller's recommendation.
RFMHC management has ensured that workforce members were re-trained on DMH Policy 500.6, Accounting of Disclosures of Protected Health Information.

- RFMHC management and supervisors were given in-house training on February 5, 2014. In attendance were Steve Hendrickson, Program Head; Antonio Banuelos, Outpatient Supervisor; Rocio Ortiz Gonzalez, FSP Supervisor; Yolanda Hernandez-Lara, PEI/School-based Supervisor; Mark Befort, CalWORKS Supervisor; and Angie Lopez, Clerical Team Leader.
- A total of 28 clinical staff was trained the following afternoon of February 6, 2014; those not present will be trained individually in their next scheduled supervision.

(Note: Ana Suarez, District Chief, Service Are #7, RFMCH, has been consulted regarding the audit, the plan of correction and the responses to the recommendations.)